



Rob Dixon CSIRT/Forensic Services Team Lead

Security Under the Covers



Recent Headlines

Pirated Media Collection

Costs Man \$46k

Suburban NYC family settles
music piracy tussle
for \$7,000 after 4 years

Graduate Student fined
\$22,500 per song.
Totaling \$675,000

Jury in RIAA Trial Slaps
\$2 Million Fine on

12-year-old Settles Music Swap Lawsuit

Minnesota Mom Hit With Fine for Illegal File Sharing

Downloading Mom
fined \$80,000 per
song

\$1.92 million

Criminals flooded several online ad networks with malicious advertisements over the weekend, causing popular Web sites such as...

**the Drudge Report, Horoscope.com
and Lyrics.com to inadvertently
attack their readers.**

**77 percent of Web sites with
malicious code are legitimate
sites**

**Court allows suit against
bank for lax security**

**How is your bank's
cyber security?**

**Linux kernels since 2001 and for which
there is already an exploit, allows users
with restricted privileges to obtain root
privileges**

Currently not patched

Security Operations Team/CSIRT

- Chris Avis – GIAC, GCFA, A+
- Rob Dixon – DHS, GIAC, GPEN, SnortCP, ESSE-D, C|HFI, TNAP, TCAP, TNEP, A+
- Mark Sizer – CISSP
- Jim Weathersbee – CISSP, CIPP/G, A+
- Jon Cain – DHS, Security +, MCSA, MCTS, ISAO-1

Contact Info

- abuse@wv.gov
- incidents@wv.gov
- soc@wv.gov
- webfiltering@wv.gov
- <http://www.technology.wv.gov/security/>

What do we do?

What do we do?

- Security Bulletins and Alert Notifications
- WV-ISAC
- Email Encryption
- Intrusion and Compliance Monitoring
- Vulnerability Management
- Network Traffic Analysis
- Web Filtering
- Incident Management
- Computer and Network Forensics
- Security Metrics

**We know what you are
doing..**

What do we monitor?

- 32 Firewalls
- 4 Intrusion sensors
- 4 Flow Collectors
- 6 HoneyPots
- 16 Domain Controllers
- 18 Other servers/devices

Why monitor all those devices?

- Login Events
- Failed Login Events
- Privilege Abuse
- Excessive Firewall Denies
- IDS Alerts
- Application Usage
- Vulnerability Information
- Policy Violations
- Illegal Software Usage

Situational Awareness

Enterprise Vision

Content Removed

Content Removed

Content Removed

Event Volume

Events - Average Events Per Second



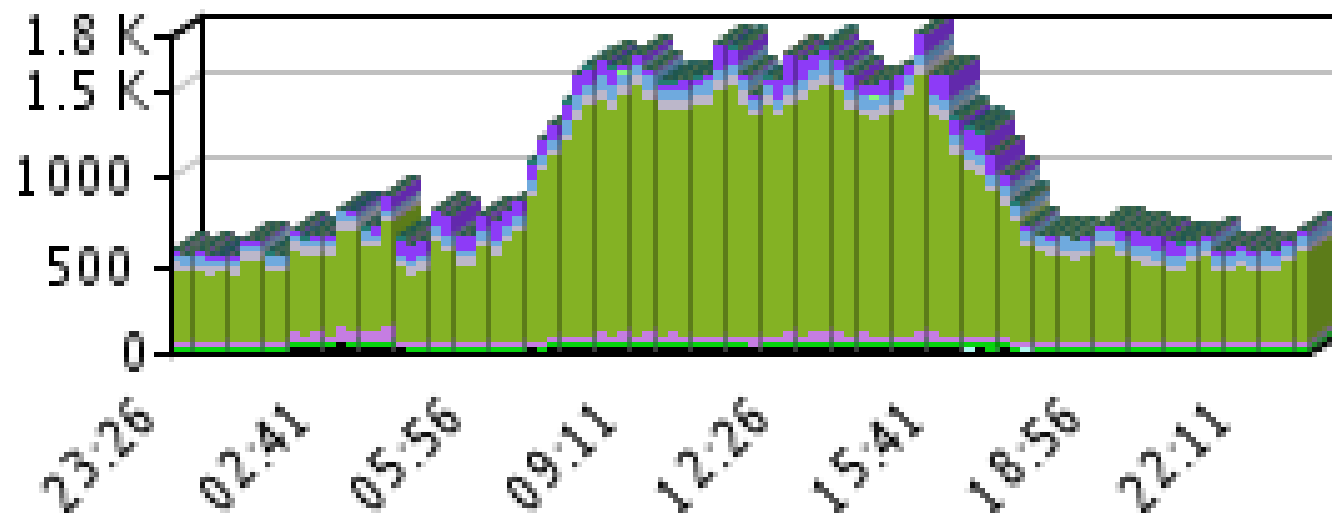
24 Hours



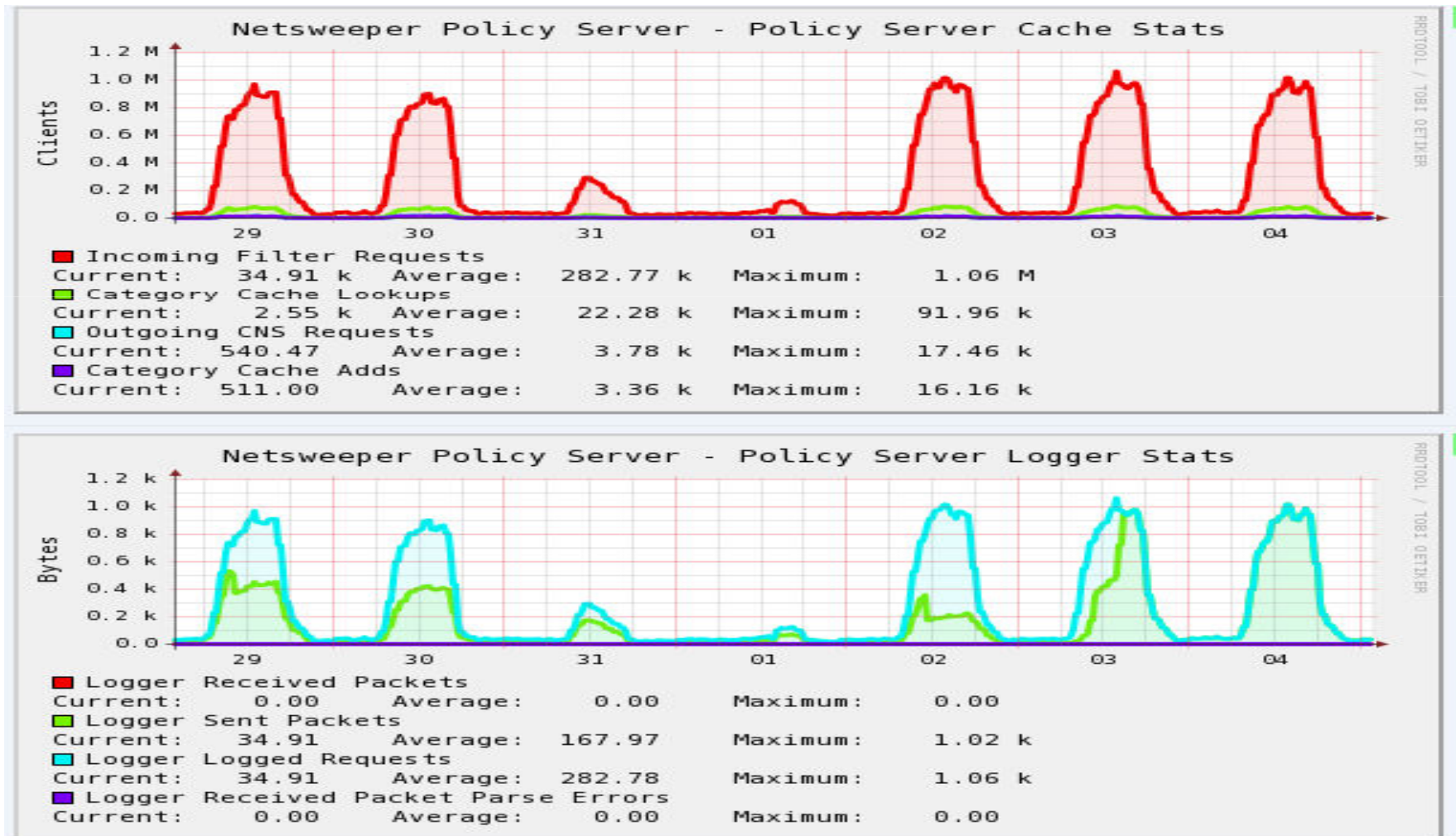
Time
Series

Line Chart

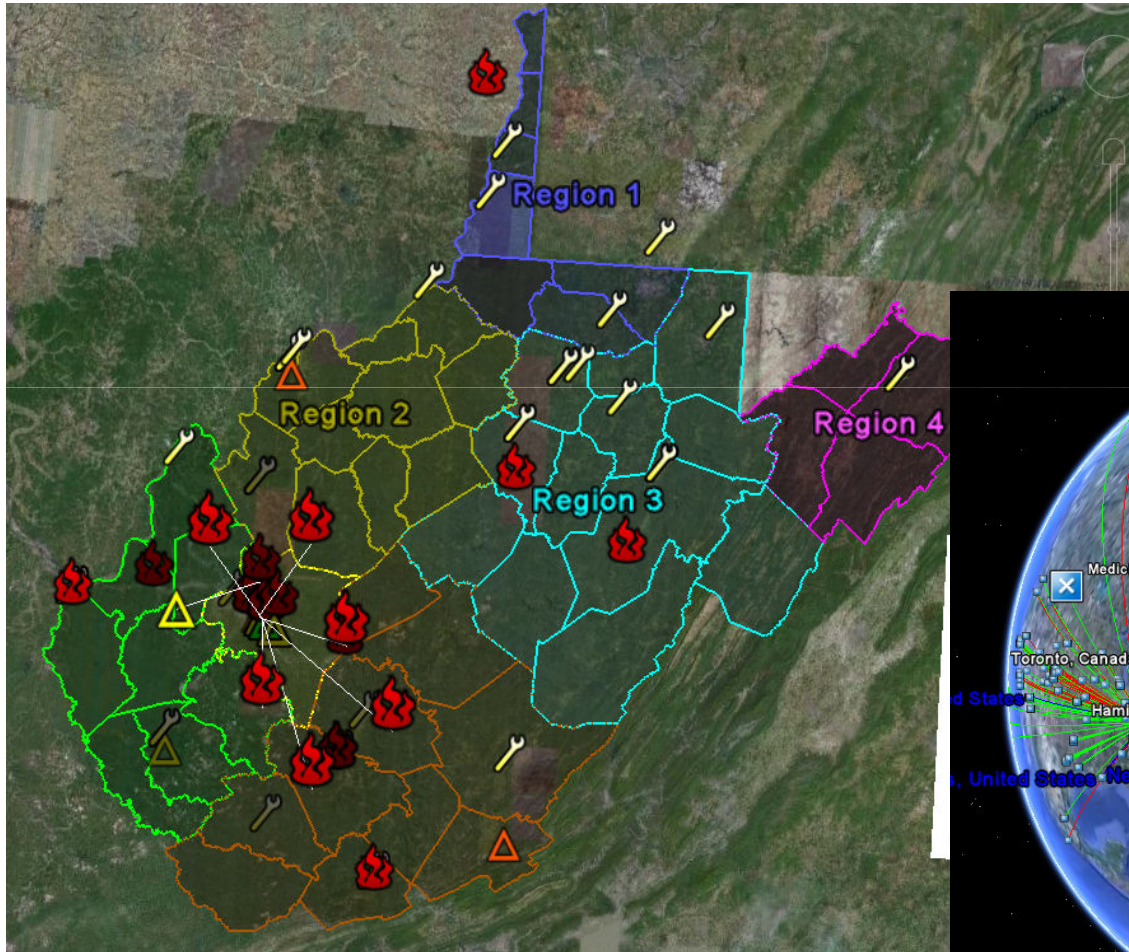
Pie Chart



Web Filtering Statistics



Google Mashups



Email

Who uses email anyway?

Total Emails Last Year

1.29 Billion

Total Viruses Last Year

261,237

Email To Virus Ratio Last Year

24:1

Total Emails Year to Date

357 Million

Total Viruses Year to Date

Over 1 Million

Email To Virus Ratio Last Year

56:1

We block stuff..

Web filtering

- 17,000 Web Surfers
- 15,799 Custom Block List
 - US-CERT
 - Discovered by SOC
- All county libraries public access computers

March

1704

April

3780

May

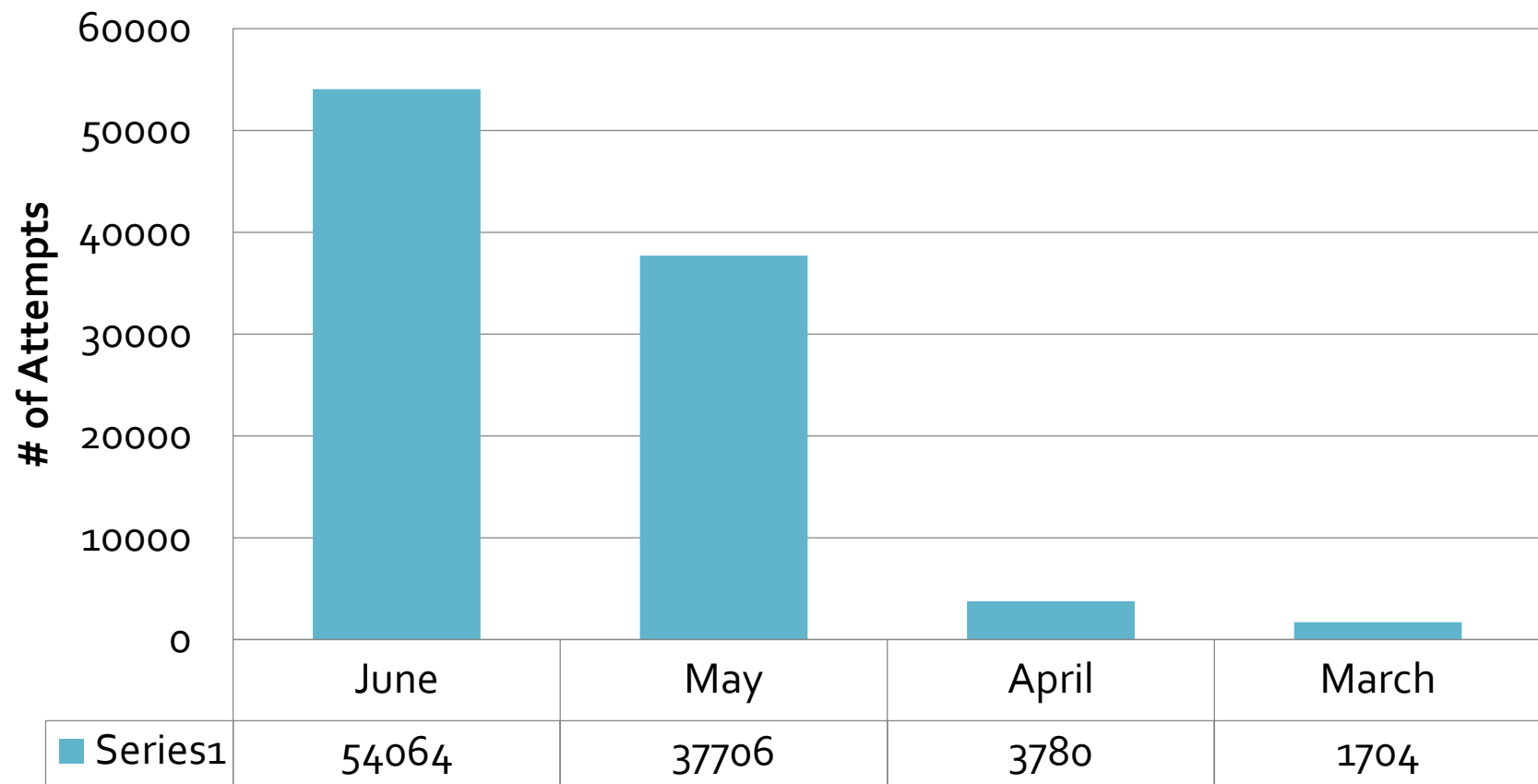
37706

June

54064

Malicious Website Attempts

Malware Connections Blocked



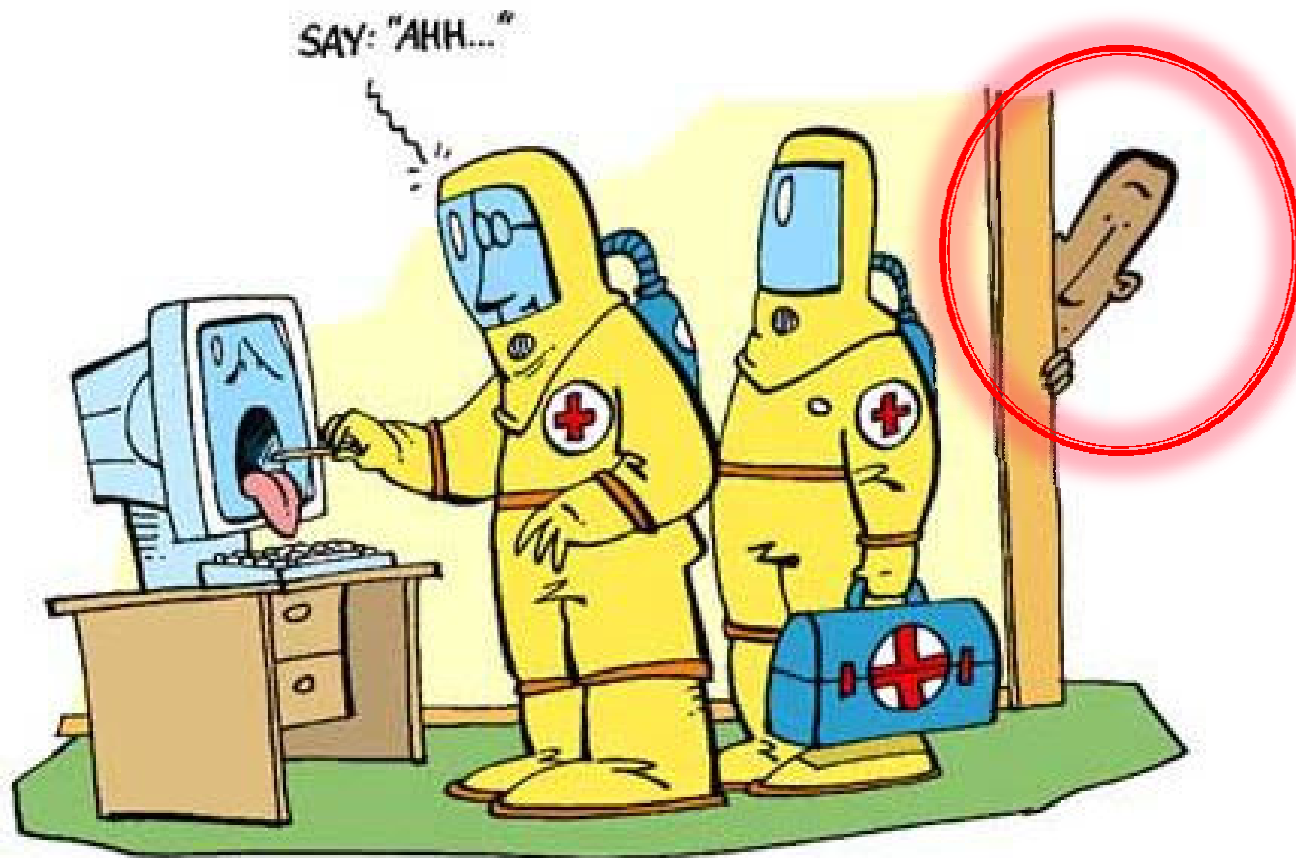
After all that?

It Still got through?

We Help Clean Up



HAZMAT Protection



I swear I didn't click on that link!!!

Anatomy of a Response

Collaboration goes a long way!

- Anti Virus
 - Reports a virus found in a PDF in a user's Temporary Internet Files
- Web Filtering
 - Find every user that accessed any file with that name
- Security Event Monitoring
 - Identifies all traffic related to the file transfer
 - Referring website
 - Resulting traffic to C&C site

Block it all!!

- Referring sites
- Malicious Content Sites
- C&Cs

Downloading MP3s is harmless

True or False??

True or False?

- Alert: Virus Found
- Computer: xxxxxxxxxxxx
- User: xxxxxxxxxxxx
- Date: xx/xx/2009
- Time: 1:08:40 PM
- Virus Name: **Trojan.Brisv.A**
- Virus Location: **E:\My Documents\Saved\80s i need love greatest hit 2009.mp3**
- Severity: **Critical**
- Source: Symantec AntiVirus Corporate Edition
- Logger: Forward from client: Auto-Protect

True or False?

- Computer: xxxxxxxxxxxx
- User: xxxxxxxxxxxx
- Date: xx/xx/2009
- Time: 8:38:49 AM
- Virus Name: **Trojan.Brisv.A**
- Virus Location: **E:\Music\The All-American Rejects - It Ends Tonight (Live from the Wiltern).mp3**

True or False?

False

Need to share!

Outreach

WV-ISAC



WV-ISAC Mission

- The West Virginia Information Sharing and Analysis Center (WV-ISAC) has been established to address the State of West Virginia's cyber security readiness and critical infrastructure coordination. The WV-ISAC currently operates out of the West Virginia Office of Technology's Cyber Security Operations Center.

Information Sharing Partners

- US Department of Homeland Security
- US-CERT (Computer Emergency Response Team)
- MS-ISAC
- Department of Military Affairs and Public Safety
- West Virginia Intelligence Fusion Center
- Joint Interagency Training and Education Center
- WV Department of Homeland Security and Emergency Management
- Critical Infrastructure Protection Task Force
- West Virginia Association of Counties
- West Virginia Municipal League

















WEST VIRGINIA
MUNICIPAL
LEAGUE



What do we share?

- Current Threat Analysis
- Incident and Threat Trends
- Cyber SARs (Suspicious Activity Reports)
- Best Practices
- Security Bulletins
- Vulnerability Advisories
- Awareness Training Materials

When do we share?

Type	Number of#
Security Bulletins	34 (Since 3/01/2008)
Multi-State Advisories	85 (Since 1-1-2008)
Newsletters	34 (1 per month since 1/1/07)

Help!!!



Phishing can be life threatening?

OFFICE OF TECHNOLOGY INFORMATION SECURITY BULLETIN

DATE ISSUED: March 26, 2008

SUBJECT: Beware of Phishing Email Threatening Violence

Summary (consistency)

Over the last couple of hours, the Office of Technology has received reports of an email phishing attempt. In this email, recipients are being warned that they have been marked for assassination. The email goes on to request that the target send a deposit of \$5000.

Below is a copy of the email:

BOGUS EMAIL *** DO NOT RESPOND *******

Sample of threatening email:

Subject: GET BACK TO ME

PREVENTION IS BETTER THAN CURE

I am very sorry for you Xxxxxx, is a pity that this is how your life is going to end as soon as you don't comply. As you can see there is no need of introducing myself to you because I don't have any business with you, my duty as I am mailing you now is just to KILL you and I have to do it as I have already been paid for that.

Someone you call a friend wants you Dead by all means, and the person have spent a lot of money on this, the person also came to us and told me that he wanted you dead and he provided us with your name ,picture and other necessary information's we needed about you. So I sent my boys to track you down and they have carried out the necessary investigation needed for the operation on you, and they have done that but I told them not to kill you that I will like to contact you and see if your life is Important to you or not since their findings shows that you are innocent.

What can you do to help?

What is a phishing attack?

Phishing is a form of social engineering. Phishing attacks use email or malicious web sites to solicit personal, often financial, information. Attackers may send email from seemingly reputable credit card company or financial institution requesting customer account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.

RECOMMENDATIONS:

- Pay careful attention to the **subject** and **from** lines. Most spam and phishing messages appear to be from legitimate sources such as your bank, a favorite online store, or a professional organization.
- **Do NOT** open emails from **UNTRUSTED** sources
- **Be cautious about opening ANY attachment or downloading any files from emails** you receive, regardless of who sent them. These files can contain viruses or other software that can weaken your computer's security.
- **DO NOT** email personal or financial information. Email is not a secure method of transmitting personal information.
- If you get an email or pop-up message that asks for personal or financial information, **DO NOT reply or click** on the link in the message. Legitimate companies don't ask for this information via email.

Why a bulletin for this email?

OFFICE OF TECHNOLOGY INFORMATION SECURITY BULLETIN

DATE ISSUED: 4/09/2009

SUBJECT: Beware of Email Phishing Scam – 'Technical Service Unit'

Over the last couple of hours, the Office of Technology has received reports of an email phishing scam. In the bogus email, recipients are being asked to enter their user name and password in order to increase their mailbox limits.

Email Message

BOGUS EMAIL ***** DO NOT RESPOND *****

From: Cpeip adminmm [mailto:Cpeip.adminmm@mineduc[dot]cl]
Sent: Thursday, April 09, 2009 1:55 PM
Subject: Technical Service Unit

Technical Service Unit

Your mailbox has exceeded the storage limit set by your administrator. You may not be able to send or receive new mail until your mailbox size is increased by your system administrator. You are required to contact your system administrator through e-mail with your

current Username: { } and
Password: { } to increase your storage limit.

System Administrator
E-mail: helpdesk-upgradeteam@live[dot]com

You will continue to receive this warning message periodically if your inbox size continues to exceed its size limit.

La informaci?n contenida en esta transmissi?n es confidencial y no puede ser usada o difundida por personas distintas a su(s) destinatario(s).

El uso no autorizado de la informaci?n contenida en este correo puede ser sancionado criminalmente de conformidad con la Ley Chilena.

Si ha recibido un correo por error, por favor destr?yalo y notifique al remitente.
El Departamento de Inform?tica del Ministerio de Educaci?n le recomienda, para el buen desempe?o de su correo, lo siguiente:

Username and password

current Username: { } and

Password: { } to increase your storage limit.

Who do we share with?

- Federal Government
- State Government
- Local Government
- Emergency Management
- Federal Law Enforcement
- State Law Enforcement
- Local Law Enforcement
- Public

Who Gets What?

- IN → WV-ISAC
 - MS-ISAC
 - US-CERT
 - Internally Developed
 - Other Partners
- WV-ISAC → OUT
 - End Users
 - System Administrators (Admins)
 - Executives
 - All at Once

Bulletins Audience

- 22,000 State Employees
- 470 Recipients across 55 counties
- 2200 Recipients Across 230 Municipalities
- 500+ other Government Contacts

25,000+ Recipients

Who can join the WV-ISAC?

- Federal Government Employees
- State Government Employees
- Local Government Employees
- Emergency Management Employees

Who should join the WV-ISAC?

- Employees responsible for IT Security
- Employees responsible for Awareness Training
- Employees responsible for IT Administration
- CIOs, CTOs, CISOs, etc

What do I (you) get?

- 24/7 Secure Access to:
 - Incident Support
 - Secure Messaging System
 - Real-time Threat Information
 - Collaboration with other WV InfoSec Professionals
 - Online Library
 - Free Information Security Training
 - Free Security Awareness Materials


RSS Feeds

http://www.technology.wv.gov/security/alerts/Pages/default.aspx

www.state.wv...

west virginia State Agency Directory | Online Services

Search technology.wv.gov

 West Virginia
Office Of Technology

PRODUCTS & SERVICES


- Overview
- Strategic Plan
- Report a Security Incident
- Monthly Newsletter
- Security Alerts
- Contact Information

Home (Technology) > Security Main Page > Security Alerts **Security Alerts**

April 1, 2009 – Conficker C Activation
Since its emergence in November 2008, the Conficker worm, also known as Downadup, has gone through several variations. The current variant of the malware, first observed March 6, 2009, is known as Conficker C

Contact Us | Site Map | Disclaimer | Services Rate Catalog

Points of Interest



`http://www.technology.wv.gov/security/alerts/`



Google


Search technology.wv.gov




Incident Reporting

**Bad news doesn't get any
better with age..**

How do I report an Incident? Demo?

 State Agency Directory | Online Services

 West Virginia
Technology



Office of Technology Incident Report Form
Incident Report Form Instructions

Enter Description here.....

Online Incident Reporting Form

Type	Number of reports
Reported via Online Reporting Form	23 (since 3/08)



WV-ISAC@WV.GOV



Rob Dixon,

GIAC, GPEN, C|HFI, ESSE-D, SnortCP, TNAP, TECP, TNCP, A+

Robert.L.Dixon@WV.GOV

304-558-5472 x 4225 (HACK)

<http://www.technology.wv.gov/security/>





Memory Erased